the 200-plus notes and bonds of varying yields and maturities that make up the market. Price information is broadcast to all approved customers, large and small, over the Bloomberg Financial Services Network. Customers can exploit this real-time awareness to initiate and complete a transaction in 2 seconds 95 percent of the time. In making the shift to network-centric operations, DMG has employed an operational architecture with three primary components:

1) a sensing capability which collects and fuses public domain information on the market;
2) a transaction capability, which contains several analytic engines which essentially perform the function of command and control, enabling the very high speed 2-second transaction timelines; and
3) an information infrastructure in the form of the Bloomberg Financial Services Network.

DMG has identified the competitive attributes required to operate more effectively in its competitive space, and it has also changed its business to reflect the value of those competitive attributes. Because of that, it is rapidly capturing market share and other firms, under intense competitive pressure, are attempting to coevolve their organizations and processes.[36]

Lessons and Insights

Integrating across the experiences of the firms that have emerged as dominant in their competitive domains, the following core themes are revealed.

1) Information technologies enable firms to create a high level of competitive awareness within their organizations and extended enterprises.
2) Networking is enabling the creation of new types of information-based relationships with and among organizations that are able to leverage increased competitive awareness.
3) Time is being compressed and, as a result, the tempo of operations is being increased.
4) The cumulative impact of better information, better distribution, and new organizational behavior provides firms with the capability to create superior value propositions for their customers and dominate their competitive space.

As we will see in the chapters that follow, these emerging themes have direct application across the spectrum of military operations. If applied wisely, they will transform DoD into an Information Age Organization that will continue to dominate its competitive domain.

Implications for Military Operations

In the last section we have seen how the Information Age is affecting organizations engaged in commercial activities, noting that these changes are driven by changes in the environments in which they operate and the capabilities they have at their disposal. These developments in the private sector are a harbinger of change and provide us with an opportunity to anticipate what factors have the potential to profoundly affect military organizations and operations. Information Age organizations achieve domination of their ecosystems by developing and exploiting information superiority. This section defines the concept of information superiority in military operations and examines the changes in the operating environment, or competitive space of military organizations, and the emerging capabilities that affect our ability to understand and influence this competitive space.

Specifically, we will look at the changed nature of our mission(s), the battlespace in which we operate, our adversaries' capabilities, our ability to sense and understand the battlespace, the capability of the weapons at our disposal, and—perhaps most important of all—our ability to command and control.

Information Superiority

JV2010 parallels the changes that are taking place in pioneering commercial organizations that are being transformed into Network-Centric Enterprises. JV2010 asserts that the operational concepts of dominant maneuver, precision engagement, full-dimensional protection, and focused logistics will be enabled by information superiority. The desired end-state is full-spectrum dominance. Information superiority, as currently defined in Joint Pub 3-13 below, addresses only the achievement of a superior information position.

> *The ability to collect, process, and disseminate an uninterrupted flow of information while exploiting and/or denying an adversary's ability to do the same.*
>
> —Joint Pub 3-13

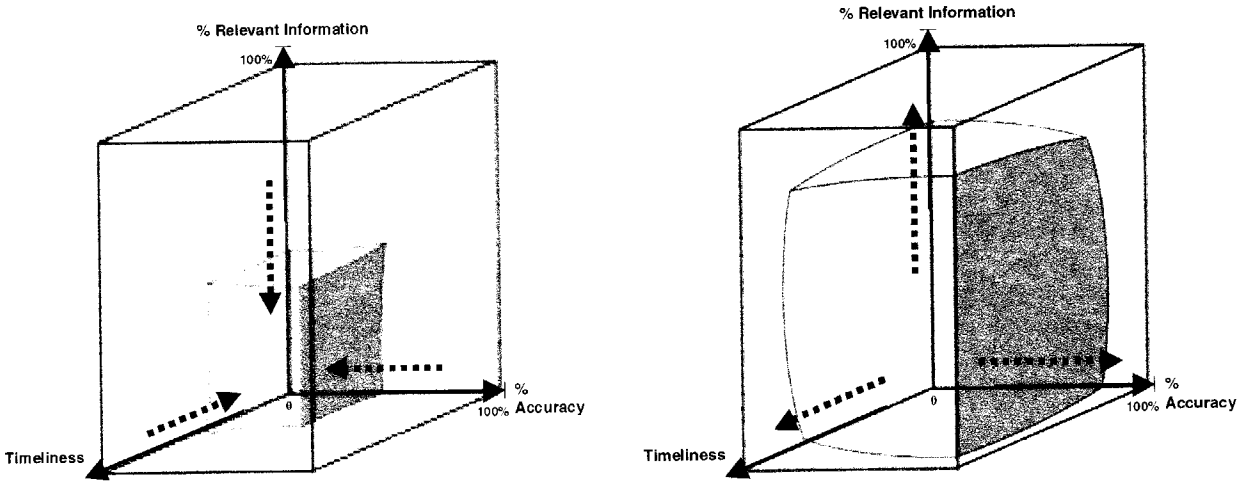
In drawing a parallel from our discussion of the commercial sector, we view *Information Superiority* in military operations as a state that is achieved when competitive advantage (e.g., full-spectrum dominance) is derived from the ability to exploit a superior information position. In military operations this superior information position is, in part, gained from information operations that protect our ability to collect, process, and disseminate an uninterrupted flow of information while exploiting and/or denying an adversary's ability to do the same.

As in the commercial sector, information has the dimensions of relevance, accuracy, and timeliness. And as in the commercial sector, the upper limit in the information domain is reached as information

relevance, accuracy, and timeliness approach 100 percent. Of course, as in the commercial sector, we may never be able to approach these limits. Figure 7 portrays a superior information position relative to a competitor in military operations. The desired effect of offensive information operations is to drive one or more components of the competitor's information "volume" towards the origin. The desired effect of defensive information operations is to keep our information "volume" from being compressed.

Figure 8 depicts the achievement of full-spectrum dominance resulting from generating and exploiting a superior information position.

Clearly, information superiority is a comparative or relative concept. Furthermore, its value is clearly derived from the military outcomes it can enable. In this sense, it is analogous to air superiority or sea control. These capabilities are not valued for themselves, but for making extended offensive and defensive actions more effective.[37] Achieving information superiority increases the speed of command preempting adversary options, creates new options, and improves the effectiveness of selected options. This promises to bring operations to a successful conclusion more rapidly at a lower cost. The result is an ability to increase the tempo of operations and to preempt or blunt adversary initiatives and options. Information superiority is generated and exploited by adopting the network-centric concepts, pioneered in the commercial sector, that allow organizations to achieve shared awareness and self-synchronization. The bottom line for value creation in military operations involves the detection,



Red Force Capability

Blue Force Capability

Figure 7. Superior Information Position Vis-À-Vis an Adversary

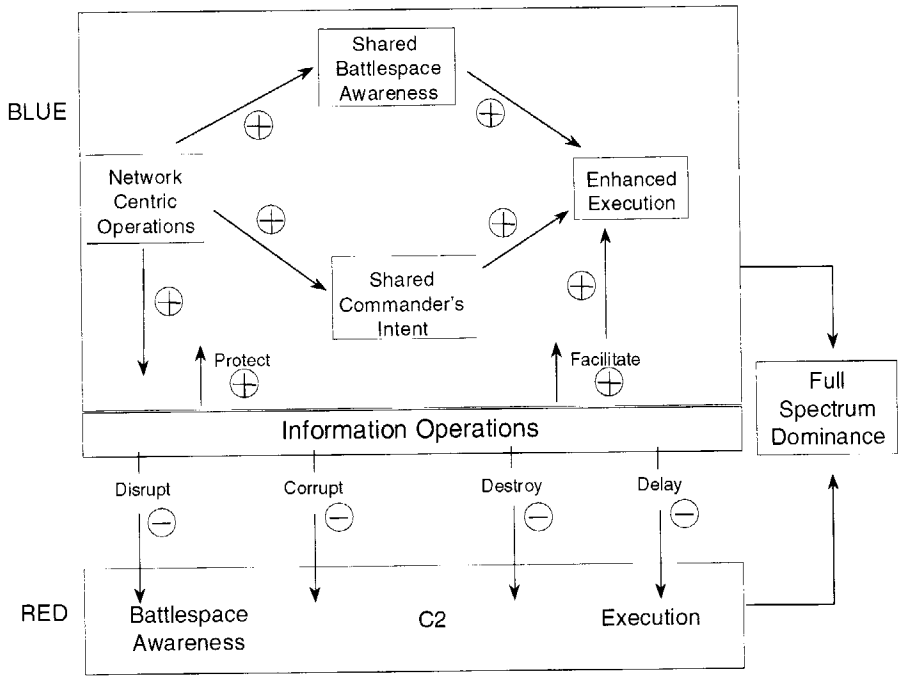


Figure 8. Full-Spectrum Dominance Enabled by Information Superiority

identification, and disposal of the most important targets at any given time. The biggest challenge lies in fleeting targets, those that are mobile and whose value is time sensitive.

What's Different about the Mission Space and the Battlespace

The mission space relevant to U.S. national security is expanding and becoming more complex. The United States, as the only superpower, has a key role to play in the post-Cold War era. Our roles and responsibilities are somewhat different from those we had in a bipolar world. Several important differences affecting military organizations and operations have already manifested themselves. The first is the increasing importance of operations other than war (OOTW) in which military organizations are being tasked to do a wide variety of non-traditional missions, from humanitarian relief to peace enforcement.[38] Second, while these differences stem from geopolitical considerations, other changes in the mission space are driven by technology. Third is the emergence of the possibility of an entirely new form of warfare, Information Warfare, or perhaps more generically, Infrastructure Warfare. Finally, asymmetrical forms of warfare have become significantly more potent with the increased lethality and accessibility of weapons of mass destruction (WMD).

Each of these changes has important implications for the types of capabilities we need and the constraints and stresses that are placed upon us. The undertaking of a wide variety of OOTW missions requires access to new organizations and information. We will need to

work closely with non-government organizations (NGOs) and private voluntary organizations (PVOs), associations that have relationships and agendas that often place constraints on their interactions with military organizations, and hence create a great deal of stress.[39] The need to operate effectively as part of a coalition requires some modifications to our most cherished notions about command and control, particularly the principle of the unity of command[40] and the ability to exchange information with others. Information operations, in its cyberwar form, has the potential to totally redefine the nature of warfare,[41] blur the boundaries between civilian and military responsibilities, provide a new set of weapons, and create new vulnerabilities. Information operations is an umbrella term that encompasses a wide variety of offensive and defensive activities. Offensive information operations is the subset of these activities that involves the use of digital weapons against digital targets anywhere in the battlespace. For example, it may be the insertion of a virus in an adversary command and control system or it may be a similar attack on an adversary's critical infrastructure systems (e.g., power, communications, public safety).

All of these changes have profound implications for the measures or indicators of success we use to assess and analyze operations. In some instances the line between war and peace and between friend, foe, and neutral is blurred beyond recognition. Asymmetric warfare presents a unique set of challenges, not the least of which is finding successful strategies for deterrence, detection, and response. Lethal weapons may become of little value in many situations when the political costs of using them far outweigh their

effects. Asymmetric warfare involves each side playing by its own set of rules that emphasize their respective strengths, while attempting to exploit an adversary's weakness. It is a far cry from the tank-on-tank battles or naval engagements of the past. This makes it very difficult to develop indications and warnings to alert us to someone preparing for war. Rather than working around the clock to produce aircraft, an adversary may be educating computer scientists or recruiting computer hackers.

If we look at these changes as a whole, it is clear that our missions have become far more complex and our challenges and adversaries less predictable. The information we need to sort things out has become, simultaneously, more diverse and more specific. Our measures of merit have also become more varied and complex, and our tool kit needs to be greatly expanded to handle more complex and varied situations. Dealing with this complexity will be a major challenge requiring us to approach problems and tasks somewhat differently.

In one sense, the battlespace of the 21st century will be defined by the mission space, and in another by the very nature of the Information Age. The term battlespace recently replaced battlefield to convey a sense that the mission environment or competitive space encompasses far more than a contiguous physical place. At the risk of oversimplification, the Information Age is changing the battlespace in three fundamental ways. The first involves the expansion of the battlefield as just mentioned. The second is in the nature of combatants in the battlespace, and the third is in its loss of privacy and remoteness. Each of these is discussed below.

While it is true that targets have always ranged from strategic to tactical, and have included the psychological as well as the physical, Information Age target sets will be expanded, and the relative priority of different kinds of targets will change. The expansion of the target sets is driven both by the growth in the variety of missions and in the possibilities created by advances in technology. The nature of OOTW or strategic information operations certainly puts some traditional targets out of bounds while placing more emphasis on others. The employment of information operations in traditional combat involves the use of new weapons against both traditional as well as new targets. For example, we will now have the option of a variety of cyber attacks on a communications router, a database, or a decision aid (to disrupt or degrade an enemy air defense asset), in addition to physical attacks on enemy air defenses. Or we could use both types of attacks in a coordinated manner to achieve the suppression of enemy air defenses. The costs, nature of the effects, lethality, collateral damage, ability to do battle damage assessment, covertness, and adversary and public responses will likely differ not only in our selection of targets, but also in the way they were attacked. This adds a whole new dimension that increases the complexity of a situation and the task of developing a response. Further, even in traditional combat situations with kinetic weapons, the improved range, lethality, and precision will tend to spread out the battlespace.

When these improvements in weapons are combined with improvements in sensors and analysis, concentrated forces will present high-value targets that will become increasingly vulnerable in the Information

Age. Furthermore, while the Information Age is making information available almost anywhere, almost anytime, and at reduced costs, it is not having the same effect on the economics of transportation for personnel and materiel.

Therefore, it will make the movement of information far less costly than the movement of physical things. Thus, the economic dynamics of the Information Age will drive solutions that leave people and machines where they are (a smaller in-theater footprint), and use information to make those in theater more effective—that is, to find ways to put them in the right place more often, and mass effects rather than forces. Only the pointy end of the spear will move on the battlefield of the future. Thus, the battlespace is extended by virtue of the increase in the number and variety of targets of interest and their dispersion.

The nature of the combatants in the battlespace of the future will of course depend upon the mission. Although civilians have been involved as victims and in supporting roles throughout history, they will play an increasingly important role in the battlespaces of the future. Again, this is driven by the nature of the missions that will be undertaken. For example, information operations may be conducted entirely in the civilian sector. OOTW involve both civilian and military organizations as participants.

To succeed in these missions requires that the actions of the military and civilian organizations be coordinated far more closely than they needed to be in traditional combat situations. This puts opposing military and civilian organizations in new juxtapositions. In addition

to having new classes of combatants present in the battlespace, their identities will be less clear. Guerrilla warfare and sabotage were examples of this in the past.

One of the greatest challenges we will face will be to ascertain the identity and location of our adversaries in the battlespaces of the future. Terrorists using real or logic bombs could strike from almost anywhere, and the distinction between a foreign threat and a domestic one will become blurred. (When does this become a military vs. a civilian problem?) Even in traditional warfare situations, one can expect that considerable efforts will be made to become stealthy and develop disguises. If what can be seen can be reliably killed, then the response will be to avoid being seen and thus the battlespace will become a place to play hide and seek.[42]

The third characteristic of the battlespace of the future is that it will no longer be private or remote. The Vietnam War was an early example of this. It was fought as much, if not more, in the living rooms of America as in the living jungles of Southeast Asia. More recently we experienced a similar visible "defeat" in Somalia. The battlespace for these operations was no longer confined to the battlefield.[43] The Information Age has changed the access that combatants and non-combatants alike have to information. This is because militaries and national security agencies no longer have exclusive control of real-time information. The commercial availability of quality images, location devices, access to vast stores of information, and high bandwidth circuits provide even the poorest nations or non-state actors with access to information recently available only to superpowers.

CNN and its competitors, combined with the Internet, make this information available to almost any interested person. Commercial satellites provide real-time images that are used to support a wide variety of tasks, including weather forecasting, oil exploration, and environmental analyses. These very same images could provide affordable information for potential adversaries.

The Information Age, by making it possible to collect and disseminate images widely, is seemingly bringing us a modern-day version of the Circus Maximus 24 hours a day, 7 days a week. To know is to get involved, and in a democracy, involvement means public debate. Learning to live with friends and foes alike looking over one's shoulder in real time will be a formidable challenge and can be expected to affect how we approach potential and real threats to national security.

With the glare of the public spotlight on everything, each individual event takes on a potential importance unlike anything in past times. This makes it necessary to rethink how we allocate decisions and how we educate and train our people. With one's adversaries having potentially increased visibility into our deliberations, decision-making processes, preparations, and operations, there is an increased risk of being outflanked or disrupted. In one sense the situation actually becomes more like chess, where everyone gets the same pieces and sees the same battlespace. The winner, of course, is the one who can make the best use of the pieces.

Obviously, we will also do what we can to obscure the board and alter the capabilities of the pieces. But none of this will work unless we can prevent our adversaries

from altering the rules of the game to their advantage, so that we have no good moves and no good outcomes.

A major effect of the fishbowl environment of the Information Age is its effect on the amount of time we have to make a decision. Highly placed decision makers around the globe have noted the greatly increased pressures upon them to react quickly to breaking events, often first finding out about these potential crises, not from their traditional sources, but from the news media. It is ironic that the Information Age, which on one hand gives us vastly increased capabilities to collect and process data that make it possible to make better and better decisions more and more quickly, is—with the other hand—reducing the time available to make decisions. Thus, the race is on. We need to either find ways to respond more quickly with quality decisions, or to find ways to extend the time for critical decisions by expediting other parts of the process.

What's Different about Sensors and Actors

Technology will, of course, vastly improve the performance of the sensors and actors we have. Moreover, we will achieve increases in performance while reducing unit costs, increasing the number of sensors and actors we can afford to buy. However significant these advances are, the real payoff will come from four other differences between the sensors and the actors of today and those of the Information Age. The first will involve a transfer of intelligence from the weapons or sensors to an information infrastructure or "infostructure," and a corresponding relocation of complexity from the platform to the network. The

technical term for this is the development of *thin clients*—entities with a minimum amount of processing and data storage capability that connect to servers. Of course, the thin clients of tomorrow will have many times the capability that current *thick* clients have today.

The second will involve the decoupling of sensors from weapons platforms, in other words, the end of stove-piping. The third will come from a decoupling of sensors and weapons platforms from actors. The fourth will be the development of new sensors to sense new types of entities and new actors to provide us with novel capabilities to damage our adversaries. Each of these is discussed below.

First, the proper distribution of intelligence among the entities of a system depends upon a number of factors related to the nature of the tasks that need to be accomplished, including the locations of the sources of information, the relative costs and reliability of computing and telecommunications, the costs of the entities themselves, the relative values of different types and levels of intelligence, and security considerations. The economics of smart weapons depend a great deal on where the smarts are located. It will be feasible in the Information Age to make relatively dumb weapons appear smart by embedding dynamic intelligence in an infostructure. The dumb/smart weapons will only need to know how to obey, not how to determine what needs to be done.

Today's smart weapons have a fairly sophisticated set of capabilities on board. This degree of intelligence enables them to be fired, perhaps to be updated with the latest information, and forgotten, leaving the

terminal phase to the smart weapon that engages the target and pursues it if necessary. Dumb/smart weapons only need to be able to navigate to a point in space and time. All other functionality would be incorporated into the infostructure. The advantages of this approach will be discussed later in the section on implications.

The second and third significant changes both involve decoupling. One involves the elimination of stove-pipe sensor weapon pairings. Information Age technologies will provide the means to achieve greater interoperability and alter the micro-economic incentives and practical considerations that often drive us towards point solutions. This is the rough equivalent of moving from producing rifles one-by-one by hand, to manufacturing them with interchangeable parts.

The other involves decoupling sensors and actors from the platforms that carry them today. Platforms serve a multitude of purposes. The Information Age provides us alternative means of achieving some of these for the first time. Among the services the platforms provide are transportation, power, integration, and connectivity to decision makers. But platforms have large footprints and are difficult to make stealthy. In addition, they are very expensive to produce, man, and defend. The economics of platforms and force structure limit the number we can buy and operate. The limited number reduces our flexibility to position them to respond to simultaneous situations and their high value increases their attractiveness as targets.

NCW has the potential to enhance the value of existing platforms by extending the effective ranges of their

sensors and weapons. Advances in technology provide the opportunity to move the functionality provided by platforms to either the infostructure, the sensors, or the actor, thus permitting us to decouple functions from traditional platforms.

The fourth change is the need to invent and deploy a host of new sensors and actors:

1) sensors designed to sense new things and maneuver in close to make distinctions among things we cannot now distinguish; and
2) actors designed to achieve new effects while at the same time becoming far more stealthy.

Information operations are the ultimate in stealth. For example, one of the greatest challenges in information operations is simply to know when one is under attack. We are in the process of working on a new class of sensors that could provide this information. These need to be developed if we are to have adequate defenses in this area.

The net result of all of these changes will be the proliferation of lower cost, independent sensors and actors that will contribute to and depend more upon distributed rather than embedded intelligence. How the capabilities of these dispersed entities will be leveraged is the subject of the next section.

Challenges and Opportunities for Command and Control

Command and control is a broad term covering a multitude of activities at all levels of an organization. Folded into this term is everything from inspiring and motivating the individuals in the organization, to setting and conveying a common sense of purpose, to assigning responsibilities, to assessing how well the organization is performing.

Command and control is inherently an iterative decision-making process, as feedback from the battlespace is incorporated into plans and corrective actions. Warfare has always been a challenging domain characterized by the importance of the endeavor, risk to life, sheer magnitude of the effort, and management of uncertainty. Our approaches to command and control have been honed over time to meet these challenges. However, the Information Age-driven changes described in the preceding sections present us with a host of new command and control challenges. In this section we will examine these challenges and catalog the opportunities for improvement.

Military operations are (should be) designed to accomplish a task or solve a problem. As in other human endeavors, often the biggest problem is recognizing that there is a problem and knowing the nature of the problem. The art of military problem formulation often involves recognizing and making distinctions between tactical and strategic problems and putting them into perspective (an overall context). The development of a campaign is the formulation of a series of interrelated problems. The campaign model

for a military operation is the essence of long-range or strategic planning.

Our current approach to developing a military campaign plan is predicated upon a fairly well understood set of relationships among events that take time to unfold. Thus, the plan can be decomposed into a series of steps, each one building in a linear fashion on the preceding steps. Our ability to deal with something as complex as a military campaign depends upon our ability to break it down into these manageable pieces. We can do so because of our ability to separate events in time and space. Organizationally, we deal at three levels—the strategic, operational, and tactical. Geographically, we deal with sectors or theaters. Functionally, we usually deal with specific jobs or tasks in a sequential manner (e.g., first we do suppression of enemy air defenses and achieve air superiority, then we attack other targets). The battlespace is thus segmented, and we can deal with smaller isolated problems, tasks, or battles.

The nature of Information Age Warfare makes it more and more difficult to operate in this reductivist fashion. Technology has compressed the space and time continuum, and political realities have collapsed the clear separations among the strategic, operational, and tactical levels by introducing more dynamic rules of engagement. The new *Circus Maximus* introduces a dose of chaos, and the Wired World makes the process nonlinear. We will find it necessary to manage larger and larger pieces, and do it more and more quickly in situations that are unlike those of former ages.

At the same time we will need to integrate orders of magnitude more sources of information provided by new armies of sensors to develop, in one way or another, a coherent picture of the battlespace, and fashion our responses in a distributed environment. This is the basic nature of the command and control challenge of the Information Age. It is not surprising that some who are beginning to understand the nature of the daunting challenge are not eager to take it on and would like the past to hold on for a bit longer. This approach ignores both the immediacy of the challenge and the potential payoff.

All of this challenges our most basic assumptions about command and control and the doctrine developed for a different time and a different problem. One of the most enduring lessons derived from the history of warfare is the degree to which fog and friction permeate the battlespace. The fog of battle is about the uncertainty associated with what is going on, while the friction of war is about the difficulty in translating the commander's intent into actions. Much of the fog of war, or what is referred to today as a lack of battlespace awareness, has resulted in our inability to tap into our collective knowledge, or the ability to assemble existing information, reconcile differences, and construct a common picture. There needs to be equal emphasis placed upon developing a current awareness of both friendly and enemy dispositions and capabilities, and in many cases, there needs to be increased emphasis on neutrals. Traditionally, the responsibilities for each of these interrelated pieces of battlespace awareness have been parsed to different organizations, resulting in significant barriers to pulling together a complete picture. The rest of the

problem is a lack of coverage resulting from limited-range sensors and their ability to discriminate.

The friction of war derives from a variant of Murphy's Law, exacerbated by the difficulty in clearly communicating information to people and resulting differences of perception. Dealing with a battlespace permeated with fog and needing to develop plans that must survive the worst of Murphy have been preeminent commander's challenges since the dawn of warfare. Command and control, as we know it, was developed to meet this challenge. Dealing with the fog and friction of war places the relative emphasis on:

1) not making a big mistake;
2) not harming one's own;
3) achieving a semblance of cohesion;
4) maximizing effectiveness; and
5) achieving economies of force.[44]

Deliberate planning, massing of forces, use of reserves, rigid doctrine, restricted information flows, and emphasis on unity of command are among the legacy of centuries of dealing with the fog and friction of war.

While the Information Age will not eliminate the fog and friction of war, it will surely significantly reduce it, or at the very least change the nature of the uncertainties. We need to rethink the concepts and practices that were born out of a different reality. We need to begin by looking at the way we currently formulate military problems and the nature of the solutions we favor. Individuals tend to formulate problems based upon their expertise and experience.

In other words, they tend to think in the box. Simply put, the Information Age is changing the box in a number of dimensions. In its most basic form, the problem box consists of an objective function (mission objectives), a set of options (courses of actions, approaches, tools), and states (enemy actions, circumstances, etc.). We have noted earlier that the Information Age has altered mission objectives, limited some earlier options, provided new options, altered the nature of the states considered through changing circumstances, and provided our potential adversaries with new capabilities.

The Information Age has also had an effect on how we solve problems and implement solutions. Solving a problem boils down to making a decision or series of decisions (selecting an alternative). In military operations, formulating and making command decisions are part of a well-understood planning process, and the implementation of these decisions is part of a well-oiled execution process.

The Information Age has changed the way we reach decisions, allocate decision responsibilities within the organization, develop options and evaluate them, and the manner in which we choose among them. This has obvious implications in how we design systems and train people. The Information Age has created an environment where collaborative decision making can be employed to increase combat power, partly because of the emergence of coalition operations, partly because of the distribution of awareness and knowledge in the battlespace, and partly because of the compression of decision timelines. This alone would be challenging enough, but the Information Age has also transformed

the problem of warfare from a series of static events to a more continuous one by greatly increasing the operating tempo of events. The result is the need for greater integration between the heretofore separate planning and execution processes, requiring more timely interactions between the two, and portents an ultimate merging of these two processes into a seamless form of command and control.

In the past the command and control process has been characterized by an iterative sequential series of steps. Various representations of this form all include sensing, fusing, understanding, deciding, conveying the decisions, and acting (execution). The cycle starts again with battlespace damage assessment (BDA).

Three such models of the command and control process are:

1) the observation, orientation, decision, action (OODA) cycle attributed to former Air Force Colonel John Boyd;
2) a model consisting of sense, process, compare, decide, and act steps, developed by Dr. Joel S. Lawson;[45]
3) the headquarters effectiveness assessment tool (HEAT) process, consisting of monitor, understand, develop alternative actions, predict, decide, and direct steps, developed by Dr. Richard E. Hayes and others at Defense Systems, Inc., in 1984.[46]

These decision or command and control loops exist at various echelons and subordinate loops are embedded accordingly. Planning is a form of decision making that exists at a headquarters level. When viewed over time, the activities at the different echelons take place sequentially, with one level executing the existing plan while another is developing the new plan. This process has evolved to the point where planning and execution are distinct activities. Efforts to speed up the process so that more responsive plans can be developed are fast approaching the laws of diminishing returns (their natural limits).

In fact the entire loop concept for command and control is becoming outdated and needs to be replaced with a new concept of command and control—one that recognizes the need to treat different types of decisions differently and recognizes a merging of the now separate planning and execution processes (sometimes called dynamic planning).

Command and control practices have evolved over time as missions and capabilities have changed. Different military establishments have taken different approaches to command and control to fit the qualities and characteristics of their organizations.[47]

Often new command and control concepts arise out of a desire to leverage new capability that provides increased information. An illustration of this is the emergence of the concept of "Command by Negation" within the U.S. Navy. In June of 1972, the U.S. Navy introduced the F-14A into the Fleet as a replacement for the F-4 as its front line Fleet air defense fighter. The F-14A had a number of significant performance

advantages over the F-4, one of which was its ability to generate a superior level of onboard situational awareness. This superior awareness was generated by the AWG-9 radar, which provided the F-14A crew with an actual target video symbol, as opposed to raw radar returns provided by the AWG-10 radar deployed on F-4s.

This superior situational awareness remained unexploited for over 6 years, as the Fleet Air Defense Mission continued to use the same command and control doctrine employed with the F-4s. This doctrine called for fighters to be directed to targets by controllers operating in E-2s and Ship Combat Information Centers with positive control enforced when available.

The potential for F-14As to generate increased combat power became apparent in 1978 during exercise *Beacon South*. During this exercise, Royal Australian Air Force pilots, employing aggressive maneuvers designed to make tracking difficult, were able to penetrate the battle group's air defenses with their F-111s. During the exercise, U.S. Navy pilots flying F-14As had the F-111s in track, but were directed away from the F-111s by a ship-based CIC controller to what turned out to be nonexistent targets. As a result of the lessons learned from this exercise, the command and control doctrine of "Vector Logic" was approved for use in the 7th Fleet. The following year, the command and control doctrine of "Command by Negation" was approved for Fleet-wide use. Finally, this doctrine provided F-14A crews with a rule set that enabled them to exploit their superior onboard situational awareness to engage targets at will unless otherwise directed by operational commanders.[48]

The above example illustrated a change in doctrine in order to take advantage of increased battlespace awareness. Sometimes, a change in the very structure of an organization is necessary in order to exploit increased awareness. The emphasis on hierarchy and other legacy concepts and practices that were needed to accommodate the fog and friction of war have remained mainstays of command and control (e.g., unity of command and coupling information flow to the command hierarchy). One basic driver of hierarchy is span of control. Traditionally, the rule of thumb for an acceptable span of control has been "5, plus or minus 2." This was based on how many relationships an individual could effectively manage. This relatively small span of control has resulted in large organizations having many levels, creating a huge middle management. Large organizations have become ponderous and sluggish by today's Information Age standards. Information flow has slowed and is reduced to a trickle of its potential. Clearly this is not acceptable in the Information Age. To break this mold we need to effectively increase the span of control. Fortunately, the Information Age gives us the tools to do so.

The characteristics of the Information Age and the nature of the missions we will undertake in the 21st century make it important that we reexamine these basic tenets. We must realize that they are not immutable laws of nature, but solutions to problems that have been refined over the years. We have seen from the lessons of recent coalition operations[49] that unity of command may be infeasible, and one may need to strive instead for unity of effort. We have seen from the lessons of fledgling Information Age

organizations that restricting information flow to the hierarchy is a losing strategy.[50] We are beginning to realize that our advances in technology promise to reduce the fog and friction of war to the point where it no longer makes sense to devote scarce resources to restrict information to the extent we have in the past. Our freedom to search for a more appropriate way to approach command and control in the Information Age is our greatest opportunity. We cannot afford to let this opportunity slip through our fingers, for our potential adversaries will most certainly not. The reason that our competitors cannot be counted on to ignore this opportunity is that it offers a non-capital intensive way to create an effective asymmetric capability, and many of these competitors are neither hampered by huge investments in legacy systems, nor the tyranny of past successes.

Implications for Future Command and Control

Starting with a clean sheet of paper, how would we describe the requirements for future command and control, and what implications do these requirements have for our approach to shaping and managing the battlespace? It should be noted that the task has been cast as managing the battlespace, not just managing our assets or forces. (The use of the term management here does not imply control, but should be read broadly enough to include influence.)

We can start by identifying what needs to be managed, noting that attention needs to be focused on the interactions among entities. First, of course, are our sensors and actors. Second is the supporting infostructure. Third, and arguably the most important

focus of command and control, is the need to manage battlespace information (information should not be confused with the systems that process and carry this information, a part of our infostructure). Fourth, are perceptions, including those of our own, our coalition partners, neutrals, and adversaries. The importance, indeed the centrality, of information is what distinguishes warfare in the Information Age from warfare in previous times. This is not to deny that information has always been important in warfare, but argues that the nature and amount of information available, and our improved ability to distribute it, will have a profound impact on the way warfare is conducted. This is discussed in detail in the next section.

We will need to make investments in all of the elements that comprise a mission capability package. This is to ensure that we have:

1) an organization and doctrine that are compatible with the concept of operations;
2) the information flows necessary to carry them out;
3) properly educated and trained personnel; and
4) a set of systems that are able to exchange and utilize the available information.

As we move to a thin client architecture, the unit costs of our sensors and actors will be reduced. These savings in unit costs will enable us to buy larger quantities of sensors and actors and to invest in the infostructure we need to support them by increasing our ability to fuse information and disseminate it intelligently.

Our next considerations are the different kinds of battlespaces we expect to encounter. Each will be driven by the characteristics of the mission, and each will have its own set of requirements that will make it necessary to tailor not only our force packages, but also our approach to command and control. One size or approach to command and control will not fit all situations. Thus, while the basic function or objective of command and control remains the same (that is, to make the most of the situation and the resources at hand), how this is accomplished (the command and control approach) will differ significantly from situation to situation. To make matters more challenging, significant differences will exist within a single battlespace, and hence there may need to be different approaches to command and control that coexist in harmony.

Finally, we need to consider the impact of the Information Age on the above as it relates to the job of command and control. The Information Age will not only have a dramatic effect on reducing the fog and friction of war, but will also permit us to consider and employ force with greater precision and granularity.

Currently the public's perception of this ability appears to be well beyond our actual abilities, which causes expectations to be somewhat unrealistic. This in turn puts considerable pressure on how we respond. The military will be judged not only by whether or not a mission was accomplished, but also whether or not it accomplished the mission with an appropriate level of force, or the minimum level to achieve the effect. Traditional military operations, conceived and conducted under the doctrine of overwhelming force, may prove to have adverse political consequences.

Thus, while our tool kit will be augmented by Information Age capabilities, our ability to use them all effectively remains unrealized. To take full advantage of these new precise tools requires that we not only achieve levels of battlespace awareness significantly higher than we have today, but also be able to deploy these tools without the large footprints needed today.

Conversely, we will want to degrade our adversaries' battlespace awareness. Requirements depend upon our ability to effectively manage battlespace information. Our current approach to command and control (and organizations) has been designed to keep the span of control within well-known human limits. As we have seen, the traditional response to the proliferation of entities requiring management is to add layers to the hierarchy, keeping the span of control manageable. This is an unacceptable response in the Information Age because it adversely affects the agility of the organization and slows the flow of information, both of which are vital to an Information Age enterprise. New approaches to command and new command arrangements are needed to effectively flatten hierarchies, free information flow (not orders) from the chain of command, and enable the enterprise to increase the speed of command to lock out adversarial options and achieve option dominance.

When sensors and actors are decoupled from one another and their supporting platforms, there will be a great increase in the number of battlespace entities that need to be managed. The pressures on Information Age organizations to reduce, not add, layers makes it important to develop new approaches

to command and control that can handle very large numbers of battlespace entities, while at the same time increasing organizational agility. The answer can be found in an altered notion of control that is inspired by the study of chaos and complexity.[51] The next section explores these issues.

The Shift to Network-Centric Operations

Although the broad tapestry of network-centric concepts is still emerging, there is clear evidence that a shift to network-centric operations has begun. The U.S. Navy's Cooperative Engagement Capability has demonstrated the increased combat power associated with the robust networking of sensors, shooters, and C2 capabilities in an Air Defense context. In the Tactical Warning and Attack Assessment mission area, Air Force Space Command's Attack and Launch Early Reporting to Theater (ALERT) capability is demonstrating the operational benefit of the robust networking of sensors in increasing battlespace awareness. The Space Based Infrared System, currently under development, exploits this same theme. In other mission areas, such as the Joint Suppression of Enemy Air Defense (JSEAD), ongoing Joint and Service experimentation explores concepts for robustly networked forces to increase combat power.[52]

Joint and Service doctrine incorporating network-centric warfighting concepts is beginning to emerge. This doctrine is being developed in order to accelerate the pace of movement of forces, maintain an unrelenting operational tempo, and decisively engage the enemy at the time and place of our choosing.[53] The operational level of war revolves around

commanders, their staffs, and their relationships with other elements of the warfighting ecosystem. The shift to network-centric operations has the potential to not only change existing command relationships, but to create new kinds of command relationships, as well as new types of commanders.[54] For example, the concept of a sensor network commander, with responsibilities for synchronizing battlespace with military operations across a Joint battlespace, has been explored in the wargaming environment.[55]

At the strategic level, senior leaders and leading military strategists are asserting the potential for the cumulative effect of closely spaced events (such as a rapid sequence of local tactical disasters, occurring over a period of hours) to dislocate and confuse an enemy to the point that his warfighting structures quickly disintegrate, and his feasible courses of action are rapidly reduced, resulting in an unequivocal military decision with minimum cost to both sides.[56] Realizing this potential will require a focused effort to work closely with allied and coalition partners as we move forward with Network Centric Warfare.[57] These developments are not lost on existing and potential adversaries, some of who are already demonstrating the capability to network their forces to increase combat power.[58]

In recent years we have witnessed a blurring of the distinctions among the levels of warfare. In particular, we have seen how what would have been considered relatively minor tactical events, or events with minor military significance (e.g., the loss of 18 American soldiers in Mogadishu, Somolia, in October 1993; the accidental bombing of the Chinese Embassy by Allied

Forces in Belgrade in May 1999 during *Operation Noble Anvil*; and the SCUD attacks against Israeli cities in the Gulf War) have had significant strategic implications. NCW, with the significantly improved capabilities that it brings to the table (in some mission areas, an order of magnitude increase in combat power), has the potential to significantly impact the outcome of military operations and enable commanders to change their operational and strategic calculus. For example, by increasing battlespace awareness, creating shared awareness, and helping to ensure that the most accurate information is made available to those who need it, situations like those that arose in Mogadishu, Belgrade, and the Gulf War can be avoided in the future, or have more favorable outcomes. Similarly, it is clear that an improved capability for performing the Joint Suppression of Enemy Air Defense Mission during *Operation Noble Anvil* would have had significant impact on the conduct of military operations.

However, this is not the only relationship between NCW and the coupling of tactical, operational, and strategic levels of war. Historically, these levels exist because of limitations in communications and span of control. As NCW lessens these constraints, we will be free to organize and operate differently. One can reasonably expect that some of the existing allocation of responsibilities among the levels of warfare will be modified as a result. This is something we need to keep our eyes on as Joint and Service experimentation proceeds.

Despite the immaturity of the Information Age and associated concepts like network-centric operations, efforts are being made to harness the opportunities they

provide to generate value in the form of increased efficiencies and enhanced combat power. If history is a guide, the future will show that current efforts are tentative first steps and incremental improvements that barely scratch the surface. In the next chapter we step back and formally define Network Centric Warfare and examine its potential to create value for military organizations.

Network Centric Warfare

Network Centric Warfare (NCW) is based upon the experiences of organizations that have successfully adapted to the changing nature of their competitive spaces in the Information Age. One of the major lessons learned is that without changes in the way an organization does business, it is not possible to fully leverage the power of information. NCW recognizes the centrality of information and its potential as a source of power. This potential is realized as a direct result of the new relationships among individuals, organizations, and processes that are developed. These new relationships create new behaviors and modes of operation. It is the cumulative impact of new relationships among warfighting organizations that are the source of increased combat power.

NCW provides a new conceptual framework with which to examine military missions, operations, and organizations. It is intended to provide a fresh perspective to help ensure that new approaches and solutions will not be constrained by outmoded ideas.

This chapter begins by defining Network Centric Warfare and explaining its fundamentals. This is followed by a discussion of the power of the network-centric approach to operations and organizations, and the manner in which this power is generated. The

chapter concludes with a look at battlespace entities through the lens of NCW.

Definition of Network Centric Warfare

NCW is about human and organizational behavior. NCW is based on adopting a new way of thinking—network-centric thinking—and applying it to military operations. NCW focuses on the combat power that can be generated from the effective linking or networking of the warfighting enterprise. It is characterized by the ability of geographically dispersed forces (consisting of entities) to create a high level of shared battlespace awareness that can be exploited via self-synchronization and other network-centric operations to achieve commanders' intent.[59] NCW supports speed of command—the conversion of superior information position to action. NCW is transparent to mission, force size, and geography. Furthermore, NCW has the potential to contribute to the coalescence of the tactical, operational, and strategic levels of war. In brief, NCW is not narrowly about technology, but broadly about an emerging military response to the Information Age.

Figure 9, The Military as a Network-Centric Enterprise, relates the basic elements necessary to generate combat power to the Network-Centric Enterprise model discussed earlier. As in the commercial sector, it all begins with infostructure. This in turn enables the creation of shared battlespace awareness and knowledge. This awareness and knowledge is leveraged by new adaptive command and control approaches and self-synchronizing forces. The "bottom line" here is increased tempo of

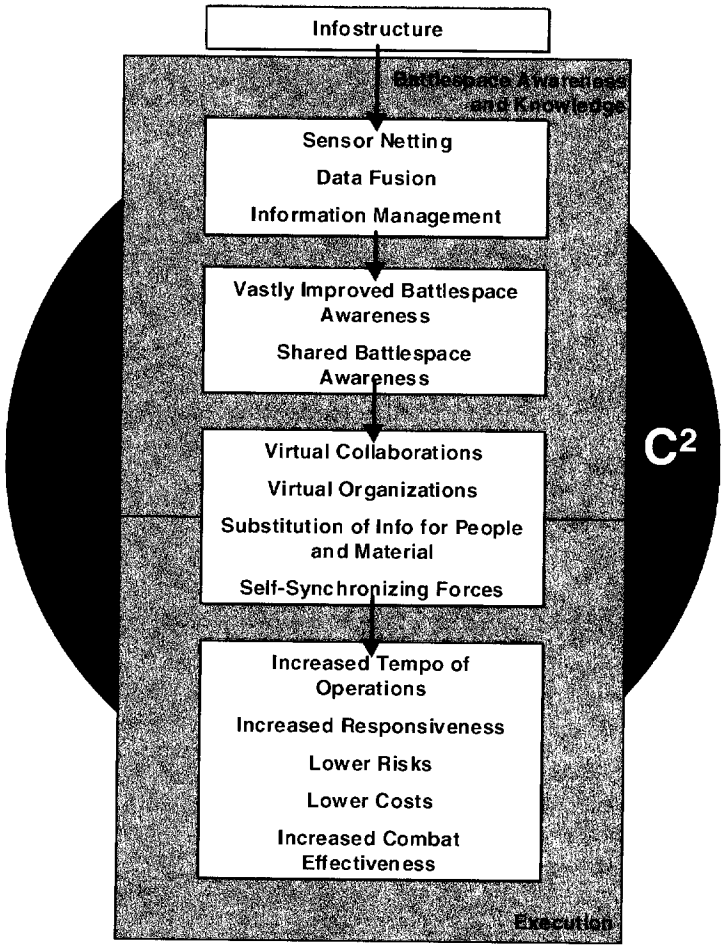


Figure 9. The Military as a Network-Centric Enterprise

operations, increased responsiveness, lower risks, lower costs, and increased combat effectiveness.

There are several key concepts in this definition that merit emphasis. The first key concept is the use of a *geographically dispersed* force. In the past, due to limitations in our ability to: 1) communicate, 2) move, and 3) project effects, forces (and their supporting elements) needed to be co-located, or in close proximity, to the enemy or to the target they were defending. As a result, a geographically dispersed force was relatively weak, and was unable to quickly respond to or mount a concentrated attack. Locational constraints also paced a force's ability to move rapidly while maintaining cohesion and logistics support. The technologies of the Information Age have made it possible to free the source of combat power from the physical location of battlespace assets or entities and may, in the future, allow forces to be more effective "on the move." Eliminating geo-locational constraints associated with combat has several inherent advantages.

It allows us to move from an approach based upon the massing of forces to one based upon the massing of effects.

As the ranges of our sensors and weapons increase and as our ability to move information rapidly improves, we are no longer geographically constrained. Hence, in order to generate a concentrated effect, it is no longer necessary to concentrate forces.

This allows us to reduce our battlespace footprint, which in turn reduces risk because we avoid

presenting the enemy with attractive, high-value targets. It also expands the concept of maneuver by reducing the need for the transportation or movement of physical objects, a very time-consuming and expensive task. With NCW, we really can have the same thing in more than one place at the same time. This is because a sensor or shooter can now be in a position to engage many different targets without having to move.

The second key concept is the fact that our force is *knowledgeable*. Empowered by knowledge, derived from a shared awareness of the battlespace and a shared understanding of commanders' intent, our forces will be able to self-synchronize, operate with a small footprint, and be more effective when operating autonomously. A knowledgeable force depends upon a steady diet of timely, accurate information, and the processing power, tools, and expertise necessary to put battlespace information into context and turn it into battlespace knowledge.

The third key concept is that there is *effective linking* achieved among entities in the battlespace. This means that:

1) dispersed and distributed entities can generate synergy, and
2) that responsibility and work can be dynamically reallocated to adapt to the situation.

Effective linking requires the establishment of a robust, high-performance information infrastructure, or *infostructure*, that provides all elements of the

warfighting enterprise with access to high-quality information services.

The effectiveness of linking mechanisms and processes affects the power coefficient or multiplier. The nature of the links that will provide the best performance under a wide range of battlespace environments and conditions is one of the key questions that needs to be addressed as we take NCW from concept to reality. A word of caution—closer linking is not necessarily better for all battlespace entities or mission circumstances. There is no intrinsic value to be had for tightly coupled links; rather, the goal is to build the configuration that creates the most effective force.

Settling on a term to describe the likely nature of warfare in the Information Age has been difficult, with each suggested term having its shortcomings. Network Centric Warfare, as we define it, is the most appropriate term that has been suggested so far because it directly, or indirectly, recognizes the essential characteristics of the revolution taking place in the commercial sector that will be manifested in warfare in the Information Age.[60] Network Centric Warfare recognizes the potential for the decoupling of sensors from actors, and each from platforms when it specifies a geographically dispersed force. It recognizes the centrality of information by specifying knowledgeable assets. NCW, by networking our forces, also focuses attention on the importance of the interactions among battlespace entities that are necessary to generate synergistic effects.

NCW, as a whole, has the characteristics necessary for coping with an increasingly important characteristic of warfare—its dynamic nature. NCW provides commanders with the flexibility to employ a broad range of command approaches from existing approaches to emerging concepts such as self-synchronization. This operational flexibility will be necessary to meet the challenges of the Information Age.

The term Network Centric Warfare also carries some baggage. By mistake, some have focused on communication networks, not on warfare or operations where the focus should rightly be. Networks are merely a means to an end; they convey "stuff" from one place to another and they are the purview of technologists. NCW does not focus on network-centric computing and communications, but rather focuses on information flows, the nature and characteristics of battlespace entities, and how they need to interact. NCW is all about deriving combat power from distributed interacting entities with significantly improved access to information. NCW reflects and incorporates the characteristics necessary for success in the Information Age—the characteristics of agility and the ability to capitalize on opportunities revealed by developing an understanding of the battlespace that is superior to that developed by an adversary.

Power of NCW

Specifically, as its name implies, NCW focuses on reaping the potential benefits of linking together—or networking—battlespace entities; that is, allowing

them to work in concert to achieve synergistic effects (but not requiring them to always operate in a linked fashion). NCW is built around the concept of sharing information and assets. Networking enables this. A network consists of nodes (entities) and the links among them. Nodes do things (sense, decide, act) and information, both as inputs to decisions and in the form of decisions themselves, is passed over links from one battlespace entity, or node, to another.

Linking battlespace entities together will greatly increase warfighting effectiveness by allowing us to get more use out of our battlespace entities. The commercial experience has shown how information can substitute for material and how to move information instead of moving people. These substitutions generate considerable savings in time and resources and result in increased value in the form of combat power for a given level of investment.

We can understand the source of increased combat associated with network-centric operations by first examining the combat power of "platforms" or "nodes" operating in a stand-alone mode. In order to successfully engage a target, all of the following must be accomplished within a certain amount of time. First, the target must be detected. Second, it must be identified. Third, the decision to engage the target must be made. Fourth, the decision must be conveyed to a weapon. Fifth, the weapon must be aimed and fired. Associated with a particular engagement is a time budget and engagement range. The time budget varies greatly as a function of whether the target is mobile or employing countermeasures. The consumption of time depends upon the ranges of the

sensors and weapons, kill radius of the weapons, time required to communicate and process information, and decision-making times required. The effective range depends upon both the range characteristics of the sensor(s) and weapons, as well as the effect of range on the consumption of time. Figure 10, Platform-Centric Shooter, portrays a platform-centric engagement where sensing and engagement capabilities reside on the same platform, and there is only limited capability for a weapons platform to engage a target based on awareness generated by other platforms. This figure describes the functional components of an engagement for a

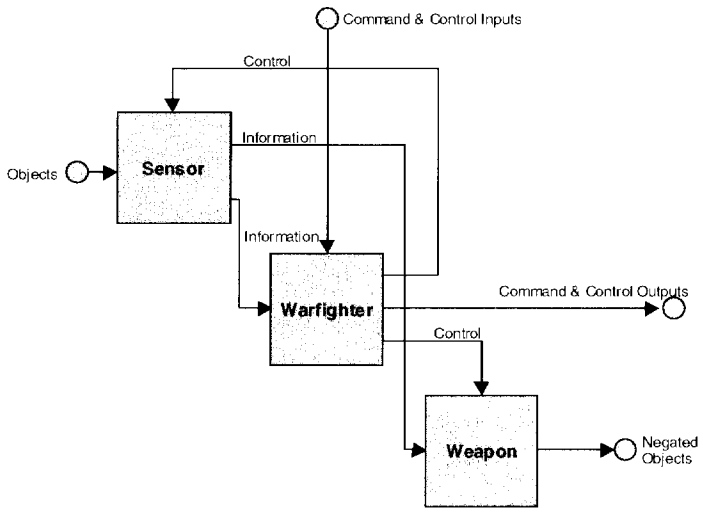


Figure 10. Platform-Centric Shooter

single warfighter on the ground, in a tank, flying an aircraft, or commanding a surface or subsurface combatant.

In combat operations, the performance capabilities of a sensor-weapon combination are governed to the first order by the geometric argument portrayed in Figure 11, Platform-Centric Engagement Envelope. In this figure, the sensing envelope is represented by a circle, and the maximum weapons employment envelope by a shaded circle. In platform-centric operations, value in the form of combat power can be created only when the platforms onboard sensor provides engagement quality awareness to the warfighter and the target is within the weapons maximum employment envelope. The effective engagement envelope is the area defined by the overlap of engagement quality awareness and the weapons maximum employment envelope. The effective engagement envelope, or E^3, is portrayed as the shaded area of the diagram. Consequently, the instantaneous combat power for a platform-centric engagement is proportional to the effective engagement envelope. As is apparent from the diagram, in platform-centric operations, combat power is often marginalized by the inability of the platform to generate engagement quality awareness at ranges greater than or equal to the maximum weapons employment envelope. This situation occurs frequently in platform-centric air engagements, as a result of the inability of an aircrew to positively identify as friend or foe the objects that they can detect and track at the full range of their sensors.

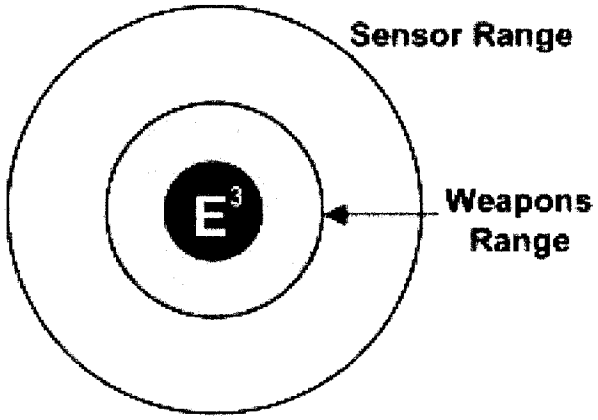


Figure 11. Platform-Centric Engagement Envelope

In the vast majority of combat operations, shooters are employed in conjunction with command and control capabilities. The operational situation that exists when platform-centric shooters are linked to a command and control node with sensing capabilities via a voice link is portrayed in Figure 12, C2 and Platform-Centric Shooters. The C2 node is capable of developing a finite level of awareness based on information provided by sensors, which may be colocated with the C2 node or external to the C2 node. In most cases, the level of awareness available to the C2 node is of sufficient quality to vector a shooter to an engagement zone, but not of sufficient quality to enable a shooter to engage directly. Furthermore, since the link between the C2 platform and the platform-centric shooter is a voice link, all information exchanges between the C2 node and shooter must take place via voice.

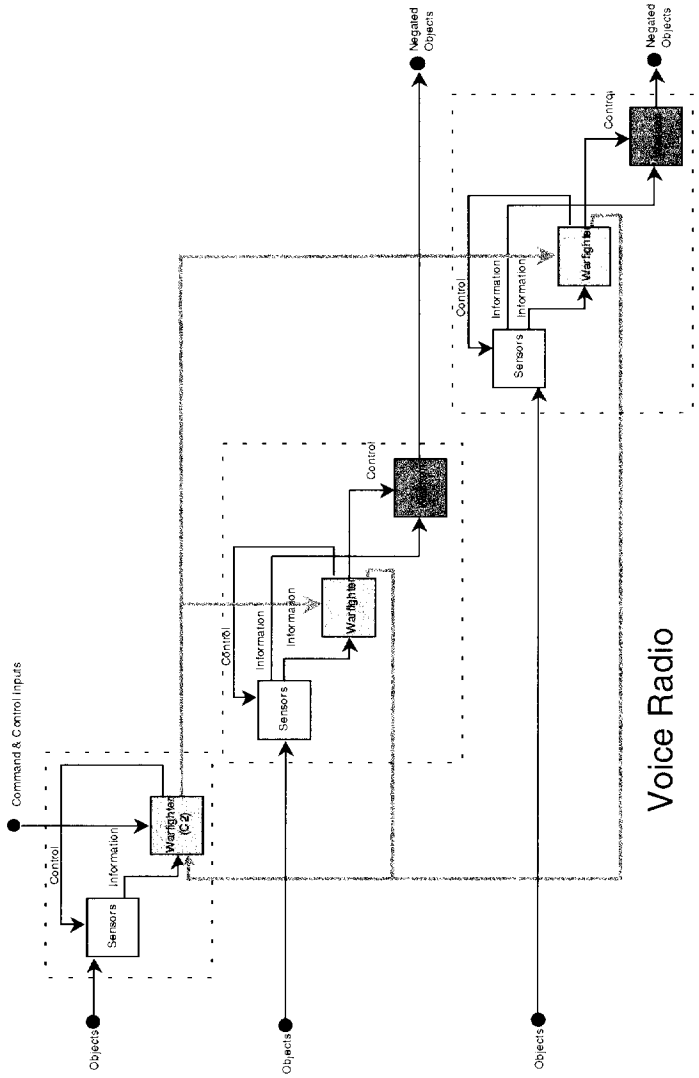


Figure 12. C2 and Platform-Centric Shooters

For example, in counter-air operations, a weapons controller onboard an E-2 Hawkeye or E-3 AWACS (Airborne Warning and Control System) does not necessarily have engagement quality awareness on all objects that it has in track. Typically, either the uncertainty associated with the position of the potential target is large or insufficient information is available to positively identify a target. Consequently, the crew of the "shooting" aircraft must employ sensors onboard the aircraft to develop engagement quality awareness (in some cases this may require performing a visual ID) and engage the target with onboard weapons. Furthermore, since all information exchanges are taking place via voice, it can be extremely difficult for the crews of the C2 node and platform-centric shooters to develop and maintain situational awareness when there are large numbers of blue and red forces operating in close proximity,

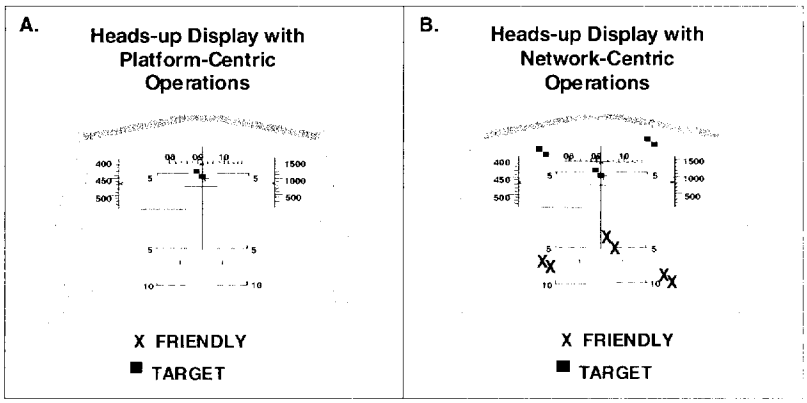


Figure 13. Platform-Centric Operations vs. Network-Centric Operations

as depicted in Figure 13A, Heads-up Display with Platform-Centric Operations.

In contrast, network-centric operations are portrayed in Figure 14. In NCW, capabilities for sensing, commanding, controlling, and engaging are robustly networked via digital data links. The source of the increased power in a network-centric operation is derived in part from the increased content, quality, and timeliness of information flowing between the nodes in the network. This increased information flow is key to enabling shared battlespace awareness, and increasing the accuracy of the information as portrayed in Figure 13B, Heads-up Display with Network-Centric Operations.

Operational experience with tactical data links provides an existence proof for the power of network-centric operations. In an experiment which compared the operational performance of Air Force F-15Cs performing counter air operations with and without data links, the Air Force found that the kill ratio increased by over 100 percent with network-centric operations. This increased combat power resulted from the significantly enhanced battlespace awareness that was provided to the pilots operating with tactical data links. Components of awareness included weapons loading of the blue force, real-time position of the blue and red force, and status of blue engagements. The net result was a significantly improved capability for observing, orienting, deciding, and acting. Findings from recent All Service Combat Identification Evaluation Team (ASCIET) Exercises reinforce these findings.